Office Automation Readiness Checklist

Use this checklist to evaluate your organisation's current automation maturity, operational discipline, and readiness for safer digital productivity.

Check each item that accurately reflects your organisation today.

Automation Strategy and Workflow Maturity

☐ 1. We have identified the most repetitive administrative tasks across our organisation.

☐ 2. We understand which workflows cause the most delays, errors, or employee frustration.

☐ 3. We evaluate automation opportunities based on business value, not just tool popularity.

☐ 4. We avoid automating unclear or poorly documented processes without improving them first.

☐ 5. We document important automated workflows and assign ownership.

AI Usage and Governance

☐ 6. We have clear guidelines for how employees may use AI tools at work.

☐ 7. Employees know what information must never be entered into public or unapproved AI platforms.

☐ 8. AI-generated content is reviewed by a human before being used in important business communication.

☐ 9. We maintain a list of approved AI tools and automation platforms.

☐ 10. Employees understand how to report AI-related concerns or accidental data exposure.

Security and Access Control

☐ 11. We review which automation tools have access to business systems and data.

☐ 12. We apply least-privilege access principles to automation platforms and connected tools.

☐ 13. Employee offboarding includes removal of access to automation tools and integrated systems.

☐ 14. We review third-party vendors before connecting them to sensitive business workflows.

☐ 15. We monitor automated workflows that affect customer data, finance, HR, or confidential information.

Communication and Operational Consistency

☐ 16. Automated emails, reminders, and notifications are reviewed for professionalism and accuracy.

☐ 17. Employees know when automated communication is appropriate and when human involvement is required.

☐ 18. We avoid excessive automated notifications that create alert fatigue.

☐ 19. We have escalation procedures when automation fails or produces incorrect results.

☐ 20. Important decisions and approvals are tracked through structured workflows rather than informal messages only.

Employee Readiness and Digital Culture

☐ 21. Employees receive training on automation, AI usage, cybersecurity awareness, and data handling.

☐ 22. Managers encourage responsible automation while maintaining oversight.

☐ 23. Employees can suggest workflow improvements through an approved process.

☐ 24. Leadership models responsible use of automation and AI tools.

☐ 25. We review automation systems periodically to ensure they remain useful, secure, and aligned with business needs.

SCORING YOUR RESULTS

Strong Maturity: 20–25 Checked Items

Your organisation demonstrates strong automation readiness.

You likely have:

- clear workflow awareness,
- practical governance,
- employee training,
- cybersecurity consideration,
- and responsible modernisation habits.

Your next step is to continue refining automation systems, reviewing workflows regularly, and strengthening digital resilience as tools evolve.

Moderate Exposure: 12–19 Checked Items

Your organisation has started building automation capability but may still have important gaps.

Common risks at this level include:

- inconsistent AI usage,
- unclear workflow ownership,
- limited documentation,
- unmanaged integrations,
- or uneven employee training.

Your next step is to prioritise policy clarity, access reviews, workflow documentation, and employee education.

High Vulnerability: 0–11 Checked Items

Your organisation may be using automation or AI informally without sufficient governance.

This can create:

- security blind spots,
- data exposure risks,
- operational inconsistency,
- employee confusion,
- and business continuity concerns.

Your next step is to establish foundational automation standards, identify high-risk workflows, review tool access, and provide practical employee guidance.